

La CNIL sanctionne Darty : les données client pas assez sécurisées

La CNIL (Commission Nationale Informatique et Libertés) a frappé fort contre les magasins Darty qui ont récemment été rachetés par le groupe Fnac : elle leur a infligé une amende pour un manquement à la sécurité des données des clients. Une amende qui est tombée le 9 janvier 2018 près d'un an après la découverte de la faille.

Darty prévenue en mars 2017 a tardé à réagir

La faille était assez importante : découverte par le site Zataz en février 2017 elle permettait d'accéder à toutes les demandes du service après-vente. Un défaut dans la sécurisation du formulaire en ligne pouvait donner accès à toutes les données personnelles des autres clients ayant demandé de l'assistance.

La CNIL a identifié le problème en vérifiant la découverte du site Zataz et en a informé Darty le 2 mars 2017 mais il semblerait que le groupe ait tardé à réagir puisque près de deux semaines plus tard, le 15 mars 2017, la CNIL a opéré un nouveau contrôle et le problème n'avait toujours pas été résolu. Un million de fiches client étaient alors toujours accessibles avec des données sensibles comme le nom, le prénom ou encore l'adresse.

Darty tente de se dédouaner, la CNIL sanctionne

Darty a tenté d'expliquer que le formulaire en question n'avait pas été développé par ses équipes mais par un prestataire tiers et que, de plus, il n'était pas utilisé. Pour la CNIL cette explication n'a pas été suffisante : le fait que le formulaire n'ait pas été développé en interne ne décharge pas l'entreprise « de son obligation de préserver la sécurité des données traitées pour son compte, en sa qualité de responsable du traitement. La société aurait dû s'assurer préalablement que les règles de paramétrage de l'outil mis en oeuvre pour son compte ne permettaient pas à des tiers non autorisés d'accéder aux données des clients » écrit la Commission dans son communiqué de presse.

Au final, donc, la CNIL a décidé de » sanctionner Darty en lui infligeant une amende de 100 000 euros le 9 janvier 2018 et en rendant publique la décision afin de « sensibiliser les internautes quant au risque pesant sur la sécurité de leurs données ».